

**BCT - UNIT 3 (Blockchain Platforms and Consensus in Blockchain) – END-SEM PYQ Answers**➤ **MAY / JUN 2023****Q1) a) Explain in details [8]****i) Bitcoin****ii) Hyperledger****i) Bitcoin**

1. Bitcoin is the **first decentralized digital currency**, introduced by *Satoshi Nakamoto* in 2008.
2. It works on a **peer-to-peer (P2P) network** without any central authority or bank.
3. All transactions are recorded on a **public blockchain ledger** visible to everyone.
4. It uses the **Proof of Work (PoW)** consensus algorithm for validating transactions.
5. **Miners** solve complex puzzles; the winner adds the block and earns bitcoins as a reward.
6. Ensures **security, transparency, and immutability** of data.
7. Faces issues like **slow transaction speed, high energy use, and scalability limits**.
8. Bitcoin laid the **foundation for blockchain technology** and inspired other cryptocurrencies.

**ii) Hyperledger**

1. Hyperledger is an **open-source blockchain project** by the *Linux Foundation* (2015).
2. It focuses on **enterprise and business applications** of blockchain.
3. Works as a **permissioned blockchain**, where only authorized members can participate.
4. Supports **modular architecture** with plug-and-play components.
5. Includes projects like **Fabric, Sawtooth, Iroha, Indy, and Burrow**.
6. **Hyperledger Fabric** is the most popular; supports **private channels** and **chaincode (smart contracts)**.
7. Provides **privacy, scalability, and controlled access** for organizations.
8. Used in **banking, supply chain, healthcare, and manufacturing** sectors.

**b) Explain types of Blockchain in details? [6]**

Blockchain technology can be divided into **four main types** based on access control and participation level.

**1. Public Blockchain**

1. Open to everyone — anyone can join, read, write, or validate transactions.
2. **Completely decentralized** with no central authority.

3. Uses consensus algorithms like **Proof of Work (PoW)** or **Proof of Stake (PoS)**.
4. Examples: **Bitcoin, Ethereum**.
5. Advantages – Transparency, security, and trustless system.
6. Limitation – Slower transactions and high energy consumption.

## 2. Private Blockchain

1. Controlled by a **single organization or entity**.
2. Only selected participants can read or write data.
3. Used for **internal business operations** where privacy is important.
4. Consensus is handled by a **central authority**.
5. Example: **Hyperledger Fabric, Corda**.
6. Advantage – High speed and privacy; Disadvantage – less decentralization.

## 3. Consortium (Federated) Blockchain

1. Controlled by a **group of organizations** rather than one entity.
2. Combines features of both public and private blockchains.
3. Members share decision-making and maintain the ledger collectively.
4. Suitable for **banking, supply chain, or government collaborations**.
5. Example: **R3 Corda, Energy Web Foundation**.
6. Advantage – More trust and efficiency among known participants.

## 4. Hybrid Blockchain

1. Mix of **public and private blockchain features**.
2. Some data is public, while sensitive data is kept private.
3. Provides **controlled access with transparency**.
4. Used in **enterprise and government projects**.
5. Example: **Dragonchain**.
6. Advantage – Flexibility and security as per requirement.

### c) Explain in details any one algorithm [4]

#### Definition:

Proof of Work (PoW) is a **consensus algorithm** used in blockchain to validate transactions and add new blocks to the chain. It ensures that all participants agree on the state of the blockchain.

#### Working Principle:

- Miners compete to solve a **complex mathematical puzzle** using computational power.
- The first miner to find the correct solution **adds the new block** to the blockchain.
- Other nodes then verify the solution before accepting the block.

**Purpose:**

- Prevents **double spending** and ensures only valid transactions are added.
- Maintains **network security and decentralization**.

**Example:**

- Used by **Bitcoin and Ethereum (before Ethereum 2.0)**.
- The miner who solves the puzzle receives a **block reward** (Bitcoin).

**Advantages:**

- Highly **secure and tamper-resistant**.
- Prevents malicious attacks due to high computational cost.

**Disadvantages:**

- Consumes **a lot of energy**.
- **Slow transaction speed** due to mining difficulty.

**Q2) a) List different consensus algorithms used in Blockchain Technology. Explain any two algorithms in detail. [8]**

**List of Consensus Algorithms:**

The major consensus algorithms used in Blockchain are:

1. **Proof of Work (PoW)**
2. **Proof of Stake (PoS)**
3. **Proof of Elapsed Time (PoET)**
4. **Proof of Activity (PoA)**
5. **Proof of Burn (PoB)**
6. **Byzantine Fault Tolerance (BFT)**

**Explanation of Any Two Algorithms (in detail):**

**(i) Proof of Work (PoW)**

1. It is the **first and most popular consensus algorithm**, used in **Bitcoin**.
2. **Miners compete** to solve complex mathematical puzzles using computational power.

3. The first miner to find the correct solution adds the **new block** to the blockchain.
4. The winner receives a **block reward** (like bitcoins).
5. Ensures **security, immutability, and decentralization** of the network.
6. **Disadvantages:** High energy consumption and slower transaction speed.

#### (ii) Proof of Stake (PoS)

1. Used in **Ethereum 2.0, Cardano**, and other modern blockchains.
2. Validators are **chosen based on the number of coins (stake)** they hold and are willing to lock.
3. No mining or heavy computation — reduces **energy usage drastically**.
4. A validator creates a block and earns a reward; dishonest validators lose their stake.
5. Ensures **faster transactions, energy efficiency, and better scalability**.
6. **Disadvantage:** Users with large stakes may get more control, reducing decentralization.

#### a) Write a note on Corda and R3 [6]

##### Corda

1. **Corda** is an **open-source blockchain platform** developed by **R3** (a consortium of financial institutions).
2. It is designed mainly for the **banking and financial services** sector.
3. Unlike public blockchains, Corda is a **permissioned blockchain**, meaning only authorized participants can join.
4. It allows **direct transactions between trusted parties**, ensuring privacy and security.
5. Corda does **not use cryptocurrency** for transaction validation — it focuses on recording and automating legal agreements.
6. It uses a **unique consensus mechanism** where only parties involved in a transaction validate it, improving efficiency.
7. Supports **smart contracts** written in **Kotlin or Java**, making it developer-friendly.
8. Ensures **high privacy, interoperability, and compliance** with business rules.

##### R3

1. **R3** is a **global financial technology (FinTech) company** that leads a consortium of over **200 banks and financial institutions**.
2. It was founded in **2014** to explore and develop blockchain solutions for enterprises.
3. **R3 developed the Corda platform** to meet enterprise needs like privacy, scalability, and regulatory compliance.
4. R3's goal is to make blockchain technology **usable in real-world finance and trade systems**.
5. It provides both **Corda Open Source** and **Corda Enterprise** versions.
6. **Corda Enterprise** offers additional features such as better security, performance, and technical support.
7. R3 helps organizations build **decentralized applications (CorDapps)** on top of Corda.
8. It focuses on industries such as **banking, healthcare, insurance, and supply chain**.

**b) Explain Byzantine General problem. [4]**

The **Byzantine Generals Problem** is a famous problem in distributed computing that explains the **difficulty of achieving consensus** among nodes when some nodes may be faulty or malicious. It highlights the challenge of ensuring all honest participants agree on a common decision despite the presence of unreliable ones.

1. Proposed by **Leslie Lamport** to describe a situation where generals of the Byzantine army must agree on whether to attack or retreat.
2. Some generals (or nodes) may be **traitors**, sending **false or conflicting messages** to others.
3. The problem shows how **trust issues** can disrupt coordination in a **distributed system**.
4. In blockchain, it represents the challenge of **achieving agreement on the same ledger** even if some participants act maliciously.
5. Blockchain networks solve this issue through **consensus algorithms** such as **Proof of Work (PoW)** or **Practical Byzantine Fault Tolerance (PBFT)**.
6. These algorithms ensure that **honest nodes** reach the same decision, maintaining the network's integrity.

The Byzantine General Problem illustrates the **trust and coordination challenges** in decentralized systems.

Blockchain overcomes this by using **robust consensus mechanisms** to ensure agreement among all honest nodes.

**➤ MAY / JUN 2024****Q1) a) Discuss following consensus algorithms used in blockchain technology.[8]****i) Proof of work****ii) Proof of activity****iii) Proof of Burn****iv) Proof of Stake****(i) Proof of Work (PoW)**

Proof of Work is the **oldest and most widely used consensus algorithm**, first implemented in **Bitcoin**. It requires participants (miners) to perform computational work to validate transactions and add new blocks.

**Key Points:**

1. Miners compete to **solve complex mathematical puzzles** using computational power.
2. The first miner to solve it adds the **new block** to the blockchain.
3. The winner receives a **block reward** (e.g., bitcoins).
4. Ensures **security, transparency, and immutability** of transactions.
5. **Drawback:** High **energy consumption** and **slow transaction speed**.

**(ii) Proof of Activity (PoA)**

Proof of Activity is a **hybrid consensus mechanism** that combines features of **Proof of Work (PoW)** and **Proof of Stake (PoS)** to improve security and energy efficiency.

**Key Points:**

1. Mining starts like PoW — miners compete to create a partially completed block.
2. Once found, the block's header is **validated by stakeholders (PoS)**.
3. Validators are selected randomly from coin holders to sign and confirm the block.
4. Both miners and validators share the **block reward**.
5. Ensures **double protection** — computational and stake-based security.

**(iii) Proof of Burn (PoB)**

Proof of Burn is a consensus method where participants **destroy (burn)** a certain number of their coins to earn the right to mine or validate new blocks.

**Key Points:**

1. “Burning” means sending coins to an **unspendable address** permanently.
2. Burning shows the miner's **commitment and investment** in the network.
3. The more coins burned, the **higher the chance** to create the next block.
4. Reduces energy waste compared to PoW but still ensures fairness.
5. Used in cryptocurrencies like **Slimcoin** and **Counterparty**.

**(iv) Proof of Stake (PoS)**

Proof of Stake is a consensus algorithm where validators are chosen based on the **amount of cryptocurrency they hold and lock (stake)** instead of computational work.

**Key Points:**

1. The higher the stake, the higher the **chance to validate** the next block.
2. **No mining** — validators are rewarded for honest participation.
3. Reduces **energy consumption** compared to PoW.
4. If a validator acts maliciously, their **staked coins are lost (slashing)**.
5. Used in **Ethereum 2.0, Cardano, and Polkadot** networks.

**b) Explain in detail [6]**

**i) Bitcoin**

**ii) Ethereum**

**iii) Hyperledger**

**i) Bitcoin**

1. Introduced by *Satoshi Nakamoto* in **2008** as the first decentralized digital currency.
2. Works on **blockchain technology** using a **peer-to-peer (P2P)** network.

3. No **central authority**; transactions are verified by miners.
4. Uses the **Proof of Work (PoW)** consensus algorithm.
5. All verified transactions are stored in a **public ledger** called the blockchain.
6. Ensures **security, transparency, and immutability** of transactions.

## ii) Ethereum

1. Developed by *Vitalik Buterin* in **2015** as a decentralized open-source blockchain platform.
2. Supports **smart contracts** and **decentralized applications (DApps)**.
3. Uses **Ether (ETH)** as its native cryptocurrency.
4. Operates on the **Ethereum Virtual Machine (EVM)** for executing contracts.
5. Initially used **Proof of Work (PoW)**; later upgraded to **Proof of Stake (PoS)** in Ethereum 2.0.
6. Commonly used for **NFTs, DeFi, and programmable blockchain applications**.

## iii) Hyperledger

1. Launched by the **Linux Foundation** in **2015** for enterprise blockchain development.
2. Designed as a **permissioned blockchain** framework for businesses.
3. Includes multiple projects like **Fabric, Sawtooth, Iroha, Indy, and Burrow**.
4. **Hyperledger Fabric** is the most popular framework.
5. Provides **modular architecture, high privacy, and scalability**.
6. Does **not use cryptocurrency** and is applied in **banking, healthcare, and supply chain** industries.

## c) Explain the concept of Bitcoin in Blockchain Technology [4 Marks]

Bitcoin is a **digital cryptocurrency** that operates on **blockchain technology** to enable secure peer-to-peer transactions without any central authority or intermediary. It was introduced by *Satoshi Nakamoto* in 2008.

### Key Points:

1. Bitcoin transactions are verified by network nodes using the **Proof of Work (PoW)** consensus algorithm.
2. All transactions are stored in a **public distributed ledger** called the **blockchain**.
3. **Miners** validate transactions and are rewarded with newly created bitcoins (block rewards).
4. Each block contains a list of verified transactions linked cryptographically to the previous block.
5. Ensures **security, transparency, and immutability** of records.
6. Used as both a **digital currency** and a **store of value** globally.

**Q2) a) Discuss the difference between Bitcoin and Ethereum. [4]**

<b>Basis</b>	<b>Bitcoin</b>	<b>Ethereum</b>
<b>Definition</b>	Bitcoin (abbreviation: BTC; sign: ₿) is a decentralized digital currency that can be transferred on the peer-to-peer bitcoin network.	Ethereum is a decentralized global software platform powered by blockchain technology. It is most commonly known for its native cryptocurrency, ether (ETH).
<b>History</b>	The word bitcoin was defined in a white paper published on 31 October 2008. The currency began use in 2009.	Ethereum was conceived in 2013 by programmer Vitalik Buterin, and then went live on 30 July 2015.
<b>Purpose</b>	The purpose of bitcoin was to replace national currencies during the financial crisis of 2008.	The purpose of Ethereum was to utilize blockchain technology for maintaining a decentralized payment network and storing computer code.
<b>Smart Contracts</b>	Although bitcoin do have smart contracts, they are not as flexible or complete as Ethereum smart contracts. Smart contracts in Bitcoin does not have all the functionality that a programming language would give them.	Ethereum allows us to create smart contracts. Smart contracts are computer codes that is stored on a blockchain and executed when the predetermined terms and conditions are met.
<b>Smart Contract Programming Language</b>	Smart contracts on Bitcoin are written in programming languages like Script, Clarity.	Smart contracts on Ethereum are written in programming languages like Solidity, Vyper, etc.
<b>Transactions</b>	Generally, bitcoin transactions are only for keeping notes.	Ethereum transactions may contain some executable code.
<b>Hash Algorithm</b>	Bitcoin runs on the <b>SHA-256</b> hash algorithm.	Ethereum runs on the <b>Keccak-256</b> hash algorithm.
<b>Consensus</b>	The Proof-of-Work (PoW) is the	The Proof-of-Stake is the consensus



<b>Basis</b>	<b>Bitcoin</b>	<b>Ethereum</b>
<b>Mechanism</b>	consensus mechanism used by the Bitcoin network.	mechanism used by Ethereum.
<b>Block Time</b>	The block time of bitcoin is 10 minutes.	The block time of Ethereum is 14 to 15 seconds.
<b>Block Limit</b>	The bitcoin blockchain has a block limit of 1 MB.	The Ethereum blockchain does not have a block limit.
<b>Popularity</b>	Bitcoin is the most popular digital currency in the market to date.	Ether, native currency of Ethereum is the second-largest cryptocurrency after bitcoin to date.
<b>Energy Consumption</b>	Energy consumption is very high.	Energy consumption is very low as compared to bitcoin
<b>Energy Consumption rate</b>	Energy consumption rate of bitcoin mining system 3.2 Million household.	Energy consumption rate of bitcoin mining system 1.2 Million household.
<b>Structure</b>	Structure of bitcoin is simple and robust.	Structure of Ethereum is complex and feature rich
<b>Rewards</b>	Miner got nearly 6.25 BTC on successfully adding new block in network.	Miner got nearly 5 BTC along with same additional rewards on successfully adding new block in network.
<b>Assets</b>	Assets of Bitcoin is BTC.	Assets of Ethereum is Ether.

**b) Explain the difference between a permissioned and permissionless consensus approach. [4]**

Points	Permissioned Consensus	Permissionless Consensus
<b>1. Access Control</b>	Only <b>authorized participants</b> can join and validate transactions.	Anyone can <b>freely join</b> and participate in the network.
<b>2. Identity</b>	Participants are <b>known and verified</b> .	Participants are <b>anonymous</b> or <b>pseudonymous</b> .
<b>3. Speed and Scalability</b>	<b>Faster</b> as it involves limited trusted nodes.	<b>Slower</b> due to more nodes and complex validation.
<b>4. Security Model</b>	Relies on <b>trust and governance</b> between known members.	Relies on <b>cryptographic proof</b> and consensus mechanisms like PoW/PoS.
<b>5. Example Platforms</b>	<b>Hyperledger Fabric, Corda</b>	<b>Bitcoin, Ethereum</b>

**c) Explain the Byzantine General Problem in the context of blockchain consensus. [4]**

1. The **Byzantine General Problem** describes a situation where **participants in a distributed system** must agree on a common decision, even if some of them act **maliciously** or **send false information**.
2. It illustrates the **difficulty of achieving consensus** when communication between nodes is unreliable or when some nodes may betray others.
3. In blockchain, this problem represents **trust issues** among nodes while verifying transactions and blocks.
4. To solve this, **consensus algorithms** like **Proof of Work (PoW)**, **Proof of Stake (PoS)**, or **Byzantine Fault Tolerance (BFT)** are used to ensure that all honest nodes agree on the same ledger state.
5. It describes a **communication failure problem** in a distributed network where some participants (generals) may send **conflicting or false messages**.
6. The generals must agree on a **common strategy (consensus)**, but if some are **traitors**, agreement becomes difficult.
7. In blockchain, it represents the **challenge of reaching agreement** on the same block or transaction when some nodes behave **maliciously**.

**d) Explain the role of IOTA in the context of the Internet of Things (IoT). [6]**

- 1) **IOTA** is a **next-generation distributed ledger technology** designed specifically for the **Internet of Things (IoT)** ecosystem.
- 2) Unlike traditional blockchains, IOTA uses a **Tangle structure**, which is a **Directed Acyclic Graph (DAG)** instead of blocks and chains.
- 3) Every new transaction in IOTA must **verify two previous transactions**, eliminating the need for miners.
- 4) This design enables **zero transaction fees**, making it suitable for **micro and machine-to-machine (M2M)** payments.
- 5) IOTA provides **high scalability** because as more devices participate, the network becomes faster and more efficient.

- 6) It ensures **data integrity, secure communication, and real-time transaction processing** among IoT devices.
- 7) IOTA helps IoT devices **exchange data and value securely** without human intervention or central control.
- 8) Example: Smart cities, energy grids, autonomous vehicles, and supply chain systems use IOTA for **secure data sharing and automated payments**.

➤ **MAY / JUN 2025**

**Q1) a) State and discuss bitcoin mining? Elaborate the functionality of miners. [8]**

- **Bitcoin mining** is the process of **verifying and adding new transactions** to the blockchain ledger using computational power.
- It involves solving a **complex mathematical puzzle** (Proof of Work) to find a hash value that meets specific network criteria.
- The miner who successfully solves the puzzle first is allowed to **add a new block** to the blockchain.
- This process ensures that all transactions are **secure, valid, and tamper-proof**.
- Mining also introduces **new bitcoins into circulation** as a **reward** for the miner's work.
- The **difficulty level** of puzzles adjusts automatically to maintain a consistent block generation time (~10 minutes).
- Mining requires **high computational power, electricity, and specialized hardware** like ASICs (Application-Specific Integrated Circuits).

**Functionality of Miners:**

- Miners **collect unconfirmed transactions** from the memory pool (mempool).
- They **verify the transaction details**, checking digital signatures and available balances.
- They **bundle valid transactions** into a candidate block.
- Each miner then **competes to solve the Proof of Work** puzzle by finding a valid hash.
- Once solved, the block is **broadcasted to the network** for validation by other nodes.
- Upon acceptance, the miner **receives block rewards and transaction fees**.
- The process ensures **network consensus, data security, and immutability** of blockchain records.

**b) Describe the features of Corda Block chain? Justify how makes it so different? Elaborate CorDapps? [9]**

**Corda Blockchain**

- **Corda** is an **open-source distributed ledger platform** developed by **R3** for use in **business and financial sectors**.

- It focuses on **privacy, interoperability, and regulatory compliance** rather than cryptocurrency.
- Corda is designed for **permissioned networks**, where participants are **known and verified entities**.

### Features of Corda Blockchain

1. **Permissioned Network** – Only authorized participants can join, ensuring **security and trust**.
2. **Privacy** – Transactions are **shared only with involved parties**, not broadcasted to the whole network.
3. **Smart Contracts** – Supports **legal and business logic** through JVM-based smart contracts.
4. **Consensus Mechanism** – Consensus is achieved only between **parties involved in a transaction**, not the entire network.
5. **Interoperability** – Different organizations can interact on a **shared network** without exposing confidential data.
6. **High Performance** – Designed for **enterprise-level scalability** and faster transaction validation.
7. **Regulatory Compliance** – Enables **auditable records** suitable for financial institutions and government systems.
8. **No Native Cryptocurrency** – Unlike Bitcoin or Ethereum, Corda doesn't have its own token or coin.

### How Corda is Different

- Corda is **not a traditional blockchain** — it doesn't use blocks or mining.
- It uses **point-to-point communication** instead of broadcasting all transactions globally.
- Focuses on **business transactions** and **legal enforceability**, not cryptocurrency exchange.
- Provides **data confidentiality** and **fine-grained access control**, unlike public blockchains.

### CorDapps (Corda Distributed Applications)

- **CorDapps** are applications built on the **Corda platform** to implement business logic.
- They consist of **flows, contracts, and states** that define how transactions are created and verified.
- Each CorDapp runs within a **Corda node** and interacts securely with other nodes.
- Used for applications in **banking, insurance, supply chain, and trade finance**.
- Example: A CorDapp can automate loan approvals, trade settlements, or KYC processes among financial institutions.

**Q2) a) Give the different types of block chain. State their advantages and disadvantages. [8]**

**1. Public Blockchain**

- Open to **everyone**; any user can join, read, write, or validate transactions.
- Works on **decentralized** consensus like **Proof of Work (PoW)** or **Proof of Stake (PoS)**.
- Example: **Bitcoin, Ethereum**.

**Advantages:**

- Fully **transparent** and **trustless**.
- High **security** due to distributed validation.

**Disadvantages:**

- **Slower** transaction speed.
- **High energy consumption** (especially in PoW).

**2. Private Blockchain**

- Controlled by a **single organization** or authority.
- Only **authorized members** can validate or participate.
- Example: **Hyperledger Fabric, Multichain**.

**Advantages:**

- **Fast** and **efficient** transaction processing.
- Better **privacy and access control**.

**Disadvantages:**

- **Centralized control** reduces transparency.
- **Limited trust** among outside participants.

**3. Consortium (Federated) Blockchain**

- Managed by a **group of organizations** instead of a single entity.
- Combines benefits of public and private blockchains.
- Example: **Corda, R3, Energy Web Foundation**.

**Advantages:**

- **Partially decentralized** and more **efficient** than public blockchain.
- Suitable for **business collaborations** and **enterprise networks**.

**Disadvantages:**

- **Setup and governance** can be complex.
- **Less transparent** than public blockchains.

**4. Hybrid Blockchain**

- A combination of **public and private** blockchain features.
- Sensitive data kept private, while general data is public.
- Example: **Dragonchain, IBM Hybrid Blockchain.**

**Advantages:**

- Offers **flexibility, security, and controlled transparency.**
- Ideal for **business–public interactions.**

**Disadvantages:**

- **Complex design** and maintenance.
- May face **integration challenges.**

**a) Illustrate 5 different types of consensus algorithm with example.[9]**

**Consensus Algorithm** ensures all nodes in a blockchain agree on a single version of truth, even without a central authority.

Here are **five major types** used in blockchain systems:

**1. Proof of Work (PoW)**

- Used in **Bitcoin** and **Litecoin**.
- Miners compete to solve a **mathematical puzzle** using computational power.
- The first miner to find the correct hash adds the block to the blockchain.
- Ensures **security and immutability** but consumes **high energy**.

**Example:** Bitcoin network uses PoW to validate and secure transactions.

**2. Proof of Stake (PoS)**

- Used in **Ethereum (after upgrade)** and **Cardano**.
- Validators are chosen based on the **amount of cryptocurrency staked** as collateral.
- Reduces energy usage compared to PoW.
- The higher the stake, the higher the chance of validating a block.

**Example:** Ethereum 2.0 uses PoS through validators staking ETH.

### 3. Proof of Burn (PoB)

- Participants **“burn” (destroy)** a certain amount of coins by sending them to an unusable address.
- This shows **commitment** and gives the right to mine new blocks.
- Helps reduce inflation and maintains network trust.

**Example:** Slimcoin and Counterparty use Proof of Burn mechanisms.

### 4. Proof of Activity (PoA)

- A **hybrid** of Proof of Work and Proof of Stake.
- Mining begins with PoW to find an empty block; then PoS is used to validate it by stakeholders.
- Ensures both **security and energy efficiency**.

**Example:** Decred blockchain implements Proof of Activity.

### 5. Proof of Elapsed Time (PoET)

- Developed by **Intel** for permissioned blockchains like **Hyperledger Sawtooth**.
- Each node waits for a **random time**; the first to finish the wait gets to create the block.
- Ensures **fairness and low energy use**, suitable for enterprise systems.

**Example:** Hyperledger Sawtooth uses PoET as its main consensus protocol.

➤ **NOV / DEC 2023**

**Q1) a) Explain any two [6]**

**i) R3**

**ii) Ethereum**

**iii) Hyperledger**

**iv) Corda**

**i) R3**

- **R3** is a **global consortium** of over 200 financial institutions developing blockchain-based solutions for business.
- It is the **organization behind the Corda platform**.
- Aims to create **secure, interoperable, and scalable distributed ledger systems** for the financial sector.

- Works on **permissioned networks** with trusted participants.
- Supports **smart contract automation** and **regulatory compliance**.
- Provides **enterprise-grade blockchain frameworks** for banking, trade finance, and insurance.

## ii) Ethereum

- An **open-source public blockchain platform** introduced by **Vitalik Buterin in 2015**.
- Supports **smart contracts** and **decentralized applications (DApps)**.
- Uses **Ether (ETH)** as its cryptocurrency.
- Consensus mechanism changed from **Proof of Work (PoW)** to **Proof of Stake (PoS)**.
- Enables developers to **create decentralized apps** using the **Solidity** programming language.
- Provides a flexible platform for **DeFi, NFTs, and enterprise solutions**.

## iii) Hyperledger

- **Hyperledger** is an **open-source project** by **Linux Foundation** for developing **enterprise-grade blockchain systems**.
- Works on **permissioned networks** with known participants.
- Provides **modular architecture** allowing multiple consensus and membership services.
- Does not use cryptocurrency; designed for **business transactions** and **data privacy**.
- Examples: **Hyperledger Fabric, Sawtooth, Indy, and Iroha**.
- Used in **banking, supply chain, and healthcare** for secure record-keeping.

## iv) Corda

- **Corda**, developed by **R3**, is a **permissioned distributed ledger** for business and finance.
- Focuses on **privacy, security, and regulatory compliance**.
- Does **not use mining** or cryptocurrency.
- Transactions are **shared only between concerned parties**, maintaining confidentiality.
- Supports **smart contracts** and **CorDapps (Corda Distributed Applications)**.
- Used in **banking, insurance, and supply chain** for secure digital agreements.

## b) Explain Proof of work with example.

**Proof of Work (PoW)** is a **consensus algorithm** used to validate transactions and secure the blockchain network.

1. It requires participants (miners) to **solve complex mathematical puzzles** using computational power.
2. The first miner to solve the puzzle **adds a new block** to the blockchain and receives a **reward**.



3. PoW ensures that adding blocks requires **real effort (work)**, making it difficult for malicious users to alter data.
4. This process maintains **network security, decentralization, and consensus** among all nodes.
5. The difficulty level automatically adjusts to keep the **block generation time** constant (e.g., 10 minutes in Bitcoin).
6. However, it consumes **high electricity and computational resources**.

#### Example:

In the **Bitcoin network**, miners compete to find a hash value (output of SHA-256 algorithm) that is **less than a target value**. They repeatedly change a random number called a **nonce** until the generated hash meets the required difficulty.

For example, if the target starts with four zeros like 0000abcd..., the miner must keep trying different nonces until the hash output starts with "0000". Once found, this proof is shared with the network, verifying the miner's effort and allowing them to add the block.

#### c) What is Byzantine General Problem? Explain its significance. [6]

The Byzantine Generals Problem explains the challenge of achieving agreement among distributed participants when some may act dishonestly or messages may fail. It highlights the difficulty of maintaining reliable communication in a decentralized network.

#### Key Points:

- It describes a scenario where generals must decide to attack or retreat, but some may send conflicting or false messages.
- The problem shows how miscommunication or malicious behavior can prevent the group from reaching a common decision.
- In blockchain, it represents the issue of ensuring all nodes agree on one valid version of the ledger.
- Consensus algorithms like Proof of Work (PoW) and PBFT are designed to solve this by allowing honest nodes to reach agreement.
- Solving the Byzantine issue ensures that even if a few nodes fail or act maliciously, the blockchain continues to operate correctly.
- This makes the system fault-tolerant, secure, and trustworthy without needing a central authority.

By overcoming this problem, blockchain achieves dependable consensus among participants, ensuring data integrity and reliability across the network.

#### Q2) a) Explain any two Blockchain platforms. [6]

##### i) Public

##### ii) Private

##### iii) Consortium

Blockchain platforms are categorized based on who can access, validate, and control the network. The main types are **Public, Private, and Consortium blockchains**, each designed for specific organizational and security requirements.

#### (i) Public Blockchain:

- A public blockchain is **open to everyone**, where any user can join, view, and participate in transactions.
- It is **fully decentralized**, with no single authority controlling the network.
- Transactions are verified through consensus algorithms like **Proof of Work (PoW)** or **Proof of Stake (PoS)**.
- Data is **transparent and immutable**, visible to all participants.
- Examples include **Bitcoin** and **Ethereum**, which ensure openness and trust among anonymous users.

Public blockchains are ideal for open ecosystems where transparency, trust, and decentralization are most important.

#### (ii) Private Blockchain:

- A private blockchain is a **restricted network** operated by a single organization or entity.
- Only **authorized participants** can access, read, or write data on the blockchain.
- Offers **better performance** and faster transaction speeds due to fewer participants.
- Ensures **privacy and control** over sensitive data within a business network.
- Example: **Hyperledger Fabric** used by enterprises for secure internal data management.

Private blockchains are suitable for organizations that require confidentiality, control, and efficient processing in a closed system.

#### (iii) Consortium Blockchain:

- A consortium blockchain is **partially decentralized**, managed by a **group of organizations** rather than one entity.
- It combines features of both public and private blockchains.
- Access is limited to selected participants, usually from trusted organizations in a specific industry.
- Consensus is achieved collectively, which improves trust and reduces single-point failure.
- Example: **R3 Corda** used in the banking sector for interbank transactions.

Consortium blockchains are preferred where multiple organizations collaborate securely while maintaining efficiency and shared control.

### b) Explain proof of stake with example. [6]

Proof of Stake (PoS) is a consensus algorithm used in blockchain networks to validate transactions and create new blocks based on the **amount of cryptocurrency a participant holds**, rather than computational power like in Proof of Work.

#### Key Points:

- In PoS, validators (participants) are chosen to create the next block **based on the number of coins they “stake”** or lock as collateral.
- The higher the stake, the higher the chances of being selected as a block validator.
- It **reduces energy consumption** as no complex mathematical puzzles are required.
- PoS discourages malicious behavior since validators risk losing their staked coins if they act dishonestly.
- It enhances **scalability and efficiency**, allowing faster transaction processing compared to Proof of Work.

- Example: **Ethereum 2.0** and **Cardano** use Proof of Stake to achieve consensus, where participants earn rewards for validating blocks.

Proof of Stake ensures energy efficiency, fairness, and security by linking the power to validate transactions directly with the participant's stake in the network.

### c) What is Consensus in Blockchain? [6]

Consensus in blockchain refers to the **mechanism through which all participants (nodes) in a distributed network agree on a single version of the truth or the state of the blockchain**. It ensures that every transaction added to the ledger is valid and verified by the majority, even without any central controlling authority.

#### Key Points:

- It allows decentralized systems to maintain data integrity and synchronization among all nodes. This ensures that all participants trust the recorded transactions.
  - Every new transaction is broadcast to all nodes in the network. These nodes validate the transaction using specific rules and reach an agreement (consensus) before adding it to the blockchain.
  - Consensus eliminates the risk of double-spending by ensuring that each digital asset can be used only once, maintaining the credibility of the blockchain.
  - Different algorithms are used to achieve consensus, such as **Proof of Work (PoW)**, **Proof of Stake (PoS)**, **Proof of Authority (PoA)**, and **Byzantine Fault Tolerance (BFT)**. Each has its own way of validating transactions and adding blocks.
  - Even if some nodes are faulty or act maliciously, the honest nodes can still maintain agreement, ensuring the blockchain remains secure and operational.
- **Key Features:** It provides **trust, transparency, and immutability**. Once data is validated through consensus and added to a block, it cannot be altered or deleted.
  - **Example:** In **Bitcoin**, consensus is achieved using Proof of Work, where miners solve cryptographic puzzles to validate transactions. In **Ethereum 2.0**, Proof of Stake is used, where validators are selected based on the number of coins staked. Consensus is therefore the **core principle** that enables blockchain to function as a reliable, decentralized, and tamper-resistant system where all participants can trust the shared ledger without needing any third-party authority.

### ➤ NOV / DEC 2024

#### Q1) a) Discuss in brief Bitcoin and Ethereum cryptocurrencies.

##### Bitcoin

Bitcoin is the first decentralized digital currency introduced by *Satoshi Nakamoto* in 2009. It operates on a peer-to-peer blockchain network that allows users to send and receive payments without relying on banks or intermediaries.

- Based on the **Proof of Work** consensus mechanism, where miners validate and add new transactions into the blockchain.
- Each transaction is verified through cryptographic hashing, ensuring transparency and security.
- Bitcoin has a **limited supply of 21 million coins**, making it scarce and resistant to inflation.
- It is widely used for **online payments, remittances, and as a digital store of value** similar to gold.
- Transactions are recorded permanently, preventing tampering or double-spending.

Hence, Bitcoin represents a secure and decentralized form of currency that transformed the concept of digital money.

### Ethereum

Ethereum is an open-source blockchain platform introduced by *Vitalik Buterin* in 2015. Unlike Bitcoin, it is designed not just for digital payments but also for creating decentralized applications and executing smart contracts.

- Uses **smart contracts**, which are self-executing programs that run automatically when conditions are met.
- The platform's native currency, **Ether (ETH)**, is used to pay transaction fees and deploy DApps.
- Initially based on Proof of Work, Ethereum has transitioned to **Proof of Stake** to reduce energy consumption.
- It supports **DeFi (Decentralized Finance)**, NFTs, and other blockchain innovations.
- Developers can build and run decentralized platforms without needing a central authority.

Thus, Ethereum extends blockchain utility beyond transactions, enabling automation and innovation across multiple sectors.

### b) Explain the following: Proof of Work, Proof of Stake, and Proof of Activity. [9]

#### Proof of Work (PoW)

Proof of Work is the original blockchain consensus mechanism used by Bitcoin. It requires participants (miners) to solve complex mathematical puzzles to validate transactions and add new blocks to the chain.

- Miners compete using computational power to find a unique hash for the next block.
- The first miner to solve the puzzle adds the block and earns a reward in cryptocurrency.
- PoW ensures network security by making attacks computationally expensive.
- However, it consumes high energy and requires specialized mining hardware.

This mechanism provides strong security but is energy-intensive and less eco-friendly.

#### Proof of Stake (PoS)

Proof of Stake is an energy-efficient alternative where validators are chosen based on the number of coins they “stake” or lock in the network.

- Instead of solving puzzles, validators are randomly selected to create new blocks.
- The chance of selection increases with the amount of cryptocurrency staked.
- Misbehavior or malicious actions can lead to loss of the staked amount (slashing).
- PoS reduces energy consumption and increases transaction speed.

Hence, PoS offers better scalability and efficiency while maintaining decentralization and trust.

### **Proof of Activity (PoA)**

Proof of Activity combines features of both Proof of Work and Proof of Stake to enhance security and fairness.

- Initially, miners use PoW to create an empty block template.
- Then, validators chosen through PoS digitally sign and confirm the block.
- This hybrid system ensures that both computational effort and stake ownership are required.
- It reduces the risk of monopoly and enhances network participation.

## **Q2) a) List and explain types of Blockchain [8]**

Blockchain technology can be classified into different types based on accessibility, participation, and control over the network. The main types are **Public**, **Private**, and **Consortium (Hybrid)** blockchains.

### **1. Public Blockchain:**

- Open to everyone — anyone can join, read, and write data on the network.
- Operates in a decentralized manner without any central authority.
- Examples include **Bitcoin** and **Ethereum**.
- Provides high transparency and security but has slower transaction speed.
- Ideal for cryptocurrencies and open applications.

### **2. Private Blockchain:**

- Controlled by a single organization or authority.
- Only authorized users can participate in the network.
- Faster and more efficient due to limited nodes.
- Commonly used in enterprises for internal record management.
- Examples include **Hyperledger Fabric** and **Corda**.

### **3. Consortium (Hybrid) Blockchain:**

- Operated by a group of organizations rather than a single entity.
- Combines features of both public and private blockchains.
- Offers partial decentralization with controlled access.
- Increases trust among multiple parties like banks or government bodies.
- Examples include **R3** and **Energy Web Foundation**.

Thus, each type of blockchain serves different purposes — public for openness, private for control, and consortium for collaboration among trusted parties.

## **b) Explain Byzantine General Problem scenario. Explain the problem and its probable consequences. [9]**

The **Byzantine General Problem** is a famous analogy used to explain the difficulty of achieving consensus in a distributed system, especially when some participants (nodes) may act maliciously or fail to communicate properly. It highlights the challenge of ensuring all honest nodes agree on a single, consistent state of the network.

**Explanation of the Problem:**

- Imagine several generals of the Byzantine army surrounding a city and communicating only through messengers.
- They must all agree on a common strategy — attack or retreat.
- However, some generals may be traitors who send false messages to create confusion.
- The loyal generals need to reach a consensus even if some messages are delayed, lost, or tampered with.
- In a blockchain context, this represents nodes that may send incorrect or inconsistent data.

**Probable Consequences:**

- Failure to reach agreement can lead to **inconsistent blockchain states** across nodes.
- Attackers could exploit disagreements to perform **double-spending** or **fraudulent transactions**.
- The network's **trust, reliability, and integrity** may be compromised.
- Transaction validation may stop or become delayed due to uncertainty among nodes.
- Overall, it can cause breakdown of coordination and system failure in decentralized environments.

Blockchain uses consensus algorithms like Proof of Work and Proof of Stake to overcome this problem, ensuring that all honest participants agree on one valid version of the ledger even when some nodes behave maliciously.

**Note: Please check and verify all answers once before referring.**